REMARKS

Claims 1-21 are pending in the present application. Reconsideration of the claims is respectfully requested.

I. Telephone Interview Summary, February 1, 2005

A telephone interview was conducted on February 1, 2005 with Examiner Chai and Examiner's Supervisor Barron with regard to features of independent claim 1. Applicants' representative submitted that Molini fails to teach classifying events as groups by aggregating events with at least one attribute within the event set as an identical value. The Examiner and Supervisor stated that further search and consideration is required before an agreement can be reached with the Applicants' representative.

II. 35 U.S.C. § 102(e), Alleged Anticipation, Claims 1-21

The Office Action rejects claims 1-21 under 35 U.S.C. § 102(e) as being allegedly anticipated by Molini (Patent Number: US 6353385 B1). This rejection is respectfully traversed.

As to claims 1-21, the Office Action states:

> As per claim 1, 8 and 15, Molini teaches a method in a data processing system for reporting security situations, comprising the steps of:
>
> logging events by storing event attributes as an event set, wherein each event set includes a source attribute, a target attribute and an event category attribute (Molini, see example, Column 5 Line 1 – 10, Column 7 Line 5 – 6 and Column 9 Line 24 – 29);
>
> classifying events as groups by aggregating events with at least one attribute within the event set as an identical value (Molini, see example, Column 8 Line 25 – 37, Column 7 Line 19 – 20, Column 6 Line 49 – 51 and Column 9 Line 30 – 35); and
>
> calculating severity levels for the groups (Molini, see example, Column Line 33);
>
> reporting a group from the groups to a user as a situation, if a severity level of the group exceeds a threshold value (Molini, see example, Column 7 Line 50 – 55 and Figure 1 Element 30 and 35).

A prior art reference anticipates the claimed invention under 35 U.S.C. § 102(e) only if every element of a claimed invention is identically shown in that single reference,

PAGE 8/14 * RCVD AT 2/7/2005 2:13:02 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/6 * DNIS:8729306 * CSID:9723857766 * DURATION (mm-ss):04-34

arranged as they are in the claims. *In re bond*, 910 F .2d 831, 832, 15 U.S.P.Q.2d 1566, 1567 (Fed Cir. 1990). All limitations of the claimed invention must be considered when determining patentability. *In re Lowry*, 32 F.3d 1579, 1582, 21 U.S.P.Q.2d 1031, 1034 (Fed Cir. 1994). Anticipation focuses on whether a claim reads on the product or process a prior art reference discloses, not on what the reference broadly teaches. *Kalman v. Kimberly-Clark Corp.*, 713 F.2d 760, 218 U.S.P.Q. 781 (Fed. Cir. 1983). Applicants respectfully submit that Molini does not teach every element of the claimed invention arranged as they are in claims 1, 8 and 15.

Independent claim 1, which is representative of claims 8 and 15 with regard to similarly recited subject matter, reads as follows:

> 1. A method in a data processing system for reporting security situations, comprising the steps of:
>
> logging events by storing event attributes as an event set, wherein each event set includes a source attribute, a target attribute and an event category attribute;
>
> classifying events as groups by aggregating events with at least one attribute within the event set as an identical value; and
>
> calculating severity levels for the groups;
>
> reporting a group from the groups to a user as a situation, if a severity level of the group exceeds a threshold value.(emphasis added)

Molini does not teach the features emphasized above. As discussed in the Abstract, Molini teaches an alarm interface system that receives intrusion alarm messages from an intrusion detection system. The alarm interface system organizes a group of the intrusion alarm messages into a time sequence. A highest priority alarm message is selected from the group. An analyzer analyzes the highest priority alarm message to extract raw locale information. The raw locale information is translated into refined locale information (e.g. a zone identifier) for inclusion in a central station-compatible data message.

However, Molini does not teach classifying events as groups by aggregating events with at least one attribute within the event set as an identical value. The Office Action alleges that Molini teaches these features at column 8, lines 25-37, column 7, 19-20, column 6, lines 49-51, and column 9, lines 30-35, which read as follows:

> The analyzer **38** the intrusion alarm messages **54** provided by the intrusion detection system **28** to determine characteristics of the attack or

PAGE 9/14 * RCVD AT 2/7/2005 2:13:02 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/6 * DNIS:8729306 * CSID:9723857766 * DURATION (mm-ss):04-34

> unauthorized intrusion upon the protected computer **16**. The locale of the attack is one example of characteristics of the attack or unauthorized intrusion. The intrusion alarm message **54** may define the locale in terms of a source indicator (e.g. source address), a destination indicator (e.g., destination address), or both. The attack of an unauthorized user terminal **12** originates at a source address. The monitoring station **22** may typically detect the attack at or near the destination address of the attack.
> (Column 8, lines 25-37)

> A quantative assessment of specific evaluative criteria used to generate the intrusion alarm messages.
> (Column 7, lines 19-20)

> In certain cases, for example, a single attack may be conducted against as many as 65,536 different ports, causing up to 65,536 separate intrusion alert messages for the same attack.
> (Column 6, lines 49-51)

> A database **18** may contain a mapping of relationships between one or more of the following: (1) a combination of a destination indicator and an origin indicator associated with a corresponding zone, (2) a destination indicator (of an electronic attack or security event) associated with a corresponding zone, and (3) an original indicator (of an electronic attack or security event) associated with a corresponding zone.
> (Column 9, lines 30-35)

In the above sections, particularly the last section, Molini merely teaches a database with a mapping of a destination address and a source address with a corresponding zone, a mapping of destination address with a corresponding zone, and a source address with a corresponding zone. However, nowhere in the above section does Molini teach that a group is classified by aggregating events that have at least one attribute within an event set as an identical value.

To the contrary, at column 8, lines 38-65, Molini teaches an analyzer that extracts these attributes from a high priority intrusion alarm message and a translator that translates the information into a zone indicator for incorporation into a central station-compatible data message. Thus, the reason behind storing the mappings in the database is to identify a zone indicator from the database given one or more attributes of a high priority intrusion alarm message. Molini does not classify messages into groups based on having at least one identical attribute value. In fact, the attributes in the database of

PAGE 10/14 * RCVD AT 2/7/2005 2:13:02 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/6 * DNIS:8729306 * CSID:9723857766 * DURATION (mm-ss):04-34

Molini are not organized by virtue of having an identical value, such as an identical source address or destination address. The attributes in the database of Molini are organized based on having a corresponding zone indicator. This is different from the presently claimed invention, as described on page 12, lines 27-28, where a group is an aggregation of events in which all of the events have at least one common element. Thus, Molini organizes messages in a database based on the attributes having a corresponding zone indicator, not based on having identical attribute values. Therefore, Molini does not teach the features of claims 1, 8, and 15 of the present invention.

In addition, Molini is only concerned with the corresponding zone identifier. At column 2, lines 15-20, Molini teaches that the presence of a zone identifier in the central station data message allows an intrusion detection system to be compatible with the context of a central alarm system that supports burglar alarms, fire alarms, or both. Therefore, Molini would not teach classifying events as groups by aggregating events with at least one attribute within the event set as an identical value, because classifying events by aggregating events with at least one attribute as an identical value does not yield a corresponding zone indicator.

While Molini teaches, at column 10, lines 44-45, organizing incoming messages into a sequential group, the messages are organized based on time sequence, as described at column 2, lines 15-17. Therefore, not only does Molini fail to teach classifying events as groups by aggregating events with at least one attribute within the event set as an identical value, Molini would not teach these features since messages are grouped based on the time they arrive.

In view of the above, Applicants respectfully submit that Molini does not teach the features of claims 1, 8 and 15. At least by virtue of their dependency on claims 1, 8 and 15 respectively, Molini does not teach or suggest the features of dependent claims 2-7, 9-14, and 16-21. Accordingly, Applicants respectfully request the withdrawal of the rejection of claims 1-21 under 35 U.S.C. § 102(e).

In addition, Molini does not teach the specific features of claims 2-7, 9-14, and 16-21. For example, with regard to claim 2, which is representative of claims 9 and 16 with regard to similarly recited subject matter, Molini does not teach that the severity levels are calculated based on at least one of the number of event sets within each of the

PAGE 11/14 * RCVD AT 2/7/2005 2:13:02 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/6 * DNIS:8729306 * CSID:9723857766 * DURATION (mm-ss):04-34

groups, the source attribute of the event sets within each of the groups, the target attribute of the event sets within each of the groups, and the event category attribute of the event sets within each of the groups.

The Office Action alleges that Molini teaches these features at column 7, lines 27-40 and at column 8, lines 48-55, which read as follows:

> The priority module **36** may estimate a danger level of an attack based on the network address targeted by the attack, the judgment of network operators, and historic occurrences of attacks and their disposition. Where possible, a priority module **36** identifies the network address of the targeted system that was targeted by the attack. The priority module determines or assigns a criticality level to the incoming alarm message according to criteria specified by a network operator of the targeted system. The criticality levels indicate a significance to a network operator concerning an attack upon a corresponding network address. To this end, the priority module **36** may contain a database **15** for storage and retrieval of criticality levels associated with the corresponding network addresses.

(Column 7, lines 27-40)

> The probability of having a valid locale for the attack may be higher if the local is based upon the both the extraction of the destination indicator and the source indicator of the attack from the highest priority intrusion alarm message **54**. Conversely, the probability of having a valid locale for the attack may be lowered if based solely on the extracted destination indicator or the extracted source indicator. The analyzer **38** communicates with a translator **40**.

(Column 8, lines 48-55)

In the above sections, Molini teaches a priority module that determines or assigns a criticality level to an incoming message based on criteria specified by a network operator of the target system. Molini also teaches that the probability of having a valid locale for the attack may be higher if both the source and destination indicators are extracted, versus solely based on extracted destination or source indicator. However, Molini does not teach or mention, in either section, a severity level calculated based on the number of event sets within each of the groups and the event category attribute of the event sets within each of the groups.

In the first section, Molini merely mentions determining a probability of having a valid locale based solely on either the source indicator or the destination indicator or

PAGE 12/14 * RCVD AT 2/7/2005 2:13:02 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/6 * DNIS:8729306 * CSID:9723857766 * DURATION (mm-ss):04-34

both. Molini does not teach or mention anything about how to calculate a severity level. In the second section, while Molini teaches how a criticality level is determined, Molini teaches that the criticality level is determined according to a criteria specified by a network operator of the target system. Molini does not determine the criticality level based on the number of event sets (messages) or the event category attribute. Therefore, Molini fails to teach the features of claims 2, 9, and 16 of the present invention.

With regard to claim 4, which is representative of claims 11 and 18 with regard to similarly recited subject matter, Molini does not teach calculating the threshold value based on at least one of the source attribute of the event sets within the group, the target attribute of the event sets within the group, the event category attribute in each event set of the group, and the number of attributes in each event set of the group that are held constant across all of the event sets in the group.

The Office Action alleges that Molini teaches these features at column 8, lines 48-55, which is reproduced above and at column 7, lines 50-63, which reads as follows:

> If the likelihood of success meets or exceeds a minimum threshold (e.g., greater than or equal to 10 percent), the priority module **36** may estimate the financial impact or severity of a successful attack on the victim (e.g., business entity) of the attack. For example, the priority module **36** may assign a lower priority to an incoming data message that indicates the detection of probing of the ports of the protected computer **16**, whereas the priority module **36** may assign a higher priority for an incoming data message that indicates an unauthorized user's illicit access of records of the internal computer **52** or the protected computer **16** because of the financial severity attendant with the illicit access.

In the above section, Molini merely teaches that the priority module estimates the impact or severity of a successful attack on the victim if the likelihood of success meets or exceeds a minimum threshold. Molini does not teach how the minimum threshold is determined. In fact, nowhere in the above section or any other section of the reference does Molini teach how to calculate a threshold value, let alone calculating a threshold value based on at least one of the source attribute of the event sets within the group, the target attribute of the event sets within the group, the event category attribute in each event set of the group, and the number of attributes in each event set of the group that are held constant across all of the event sets in the group, as recited in claims 4, 11 and 18 of the present invention.

PAGE 13/14 * RCVD AT 2/7/2005 2:13:02 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/6 * DNIS:8729306 * CSID:9723857766 * DURATION (mm-ss):04-34

In view of the above, in addition to their dependency on independent claims 1, 8, and 15, Applicants respectfully submit that Molini also fails to teach the specific features of claims 2-7, 9-14, and 16-21 of the present invention. Accordingly, Applicants respectfully request the withdrawal of rejection of claims 2-7, 9-14, and 16-21 under 35 U.S.C. § 102(e).

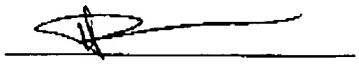
III. Conclusion

It is respectfully urged that the subject application is patentable over the cited reference and is now in condition for allowance.

The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: Feb- 7, 2005

Respectfully submitted,



Wing Yan Mok
Reg. No. 56,237
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 385-8777
Agent for Applicants

PAGE 14/14 * RCVD AT 2/7/2005 2:13:02 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/6 * DNIS:8729306 * CSID:9723857766 * DURATION (mm-ss):04-34